ECONOMIC DEVELOPMENT ADMINISTRATION

Malware Infections on EDA's Systems Were Overstated and the Disruption of IT Operations Was Unwarranted

FINAL REPORT NO. OIG-13-027-A
JUNE 26, 2013

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

FOR PUBLIC RELEASE

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

June 26, 2013

MEMORANDUM FOR: Matthew Erskine
Deputy Assistant Secretary of Commerce
for Economic Development
Economic Development Administration

Simon Szykman
Chief Information Officer

Allen Crawley

FROM: Allen Crawley
Assistant Inspector General for Systems Acquisition
and IT Security

SUBJECT: *Malware Infections on EDA's Systems Were Overstated and the Disruption of IT Operations Was Unwarranted*
Final Report No. OIG-13-027-A

Attached is the final report of our audit of EDA's information security program and cyber incident response. In accordance with the Federal Information Security Management Act, we evaluated EDA's incident response and recovery activities in relation to EDA's fiscal year 2012 cyber incident. We (1) assessed the effectiveness of EDA's IT security program, (2) determined the significant factors that contributed to its incident, and (3) evaluated both completed and planned activities to recover its information systems to support critical operational requirements.

We found (1) EDA based its critical incident response decisions on inaccurate information, (2) deficiencies in the Department's incident response program impeded EDA's incident response, and (3) misdirected planning efforts hindered EDA's IT system recovery.

In response to the draft audit report, EDA and the CIO concurred with all of our recommendations. We summarized the responses in the report and included the full response in the appendixes. We will post this report on the OIG website pursuant to section 8L of the Inspector General Act of 1978, as amended.

Under Department Administrative Order 213-5, you have 60 calendar days from the date of this memorandum to submit an audit action plan to us. The plan should outline actions you propose to take to address each recommendation.

We appreciate the cooperation and courtesies extended to us by your staff during our audit. Please direct any inquiries regarding this report to me at (202) 482-1855 and refer to the report title in all correspondence.

Attachment

cc: Thomas Guevara, Deputy Assistant Secretary for Regional Affairs, EDA
Rod Turk, Director, Office of Cyber Security, and Chief Information Security Officer
Chuck Benjamin, Chief Information Officer, EDA
Deborah Neff, Audit Liaison, EDA
Cara Huang, Audit Liaison, Office of the Chief Information Officer

Report In Brief

JUNE 26, 2013

Background

The Economic Development Administration's (EDA's) mission is to lead the federal economic development agenda by promoting innovation and competitiveness, thus preparing American regions for growth and success in the worldwide economy. To fulfill its mission, EDA uses six regional offices to provide services specific to each region's needs.

In accordance with the Federal Information Security Management Act of 2002 (FISMA), we evaluated EDA's incident response and recovery activities in relation to EDA's fiscal year 2012 cyber incident.

Why We Did This Review

On December 6, 2011, the Department of Homeland Security (DHS) notified the Department of Commerce that it detected a potential malware infection within the Department's systems. The Department determined the infected components resided within IT systems operating on the Herbert C. Hoover Building (HCHB) network and informed EDA and another agency of a potential infection in their IT systems.

On January 24, 2012—believing it had a widespread malware infection—EDA requested the Department isolate its IT systems from the HCHB network. This action resulted in the termination of EDA's operational capabilities for enterprise e-mail and Web site access, as well as regional office access to database applications and information residing on servers connected to the HCHB network.

Given the Department's limited incident response capabilities and the perceived extent of the malware infection, the Department and EDA decided to augment the Department's incident response team. Additional incident response support was provided by DHS, the Department of Energy, the National Institute of Standards and Technology, and the National Security Agency, as well as a cybersecurity contractor. In early February 2012, EDA entered into an agreement with the Census Bureau to provide an interim e-mail capability, Internet access to EDA staff, and Census Bureau surplus laptops for EDA staff.

ECONOMIC DEVELOPMENT ADMINISTRATION

Malware Infections on EDA's Systems Were Overstated and the Disruption of IT Operations Was Unwarranted

OIG-13-027-A

WHAT WE FOUND

Reviewing EDA's IT security program and the events surrounding its December 2011 cyber incident and recovery efforts, we found that:

EDA Based Its Critical Cyber-Incident Response Decisions on Inaccurate Information. Believing (a) the incident resulted in a widespread malware infection possibly propagating within its systems and (b) its widespread malware infection could spread to other bureaus if its IT systems remained connected to the network, EDA decided to isolate its IT systems from the HCHB network and destroy IT components to ensure that a potential infection could not persist. However, OIG found neither evidence of a widespread malware infection nor support for EDA's decision to isolate its IT systems from the HCHB network.

Deficiencies in the Department's Incident Response Program Impeded EDA's Incident Response. These deficiencies significantly contributed to EDA's inaccurate belief that it experienced a widespread malware infection. Consequently, the Department of Commerce Computer Incident Response Team (DOC CIRT) and EDA propagated inaccurate information that went unidentified for months after EDA's incident. We found that DOC CIRT's incident handlers did not follow the Department's incident response procedures, that its handler for EDA's incident did not have the requisite experience or qualifications, and that DOC CIRT did not adequately coordinate incident response activities.

Misdirected Efforts Hindered EDA's IT System Recovery. With its incorrect interpretation of recovery recommendations, EDA focused its recovery efforts on replacing its IT infrastructure and redesigning its business applications. EDA should have concentrated its resources on quickly and fully recovering its IT systems (e.g., critical business applications) to ensure its operational capabilities. Our review of EDA's recovery activities found that (a) EDA decided to replace its entire IT infrastructure based on its incorrect interpretation of recovery recommendations and (b) EDA's recovery efforts were unnecessary.

The Department, using already existing shared IT services, returned EDA's systems to their former operational capabilities (except for access to another Departmental agency's financial system) in just over 5 weeks of starting its effort.

WHAT WE RECOMMEND

We recommend that the Deputy Assistant Secretary for EDA:

1. Identify EDA's areas of IT responsibility and ensure the implementation of required security measures.
2. Determine whether EDA can reduce its IT budget and staff expenditures, through the increased efficiencies of EDA's involvement in the Department's shared services.
3. Ensure that EDA does not destroy additional IT inventory that was taken out of service as a result of this cyber incident.

We recommend that the Department's Chief Information Officer:

1. Ensure DOC CIRT can appropriately and effectively respond to future cyber incidents.
2. Ensure incident response procedures clearly define DOC CIRT as the incident response coordinator for the bureaus relying on DOC CIRT's incident response services.
3. Ensure that DOC CIRT management has proper oversight and involvement in cyber incidents to ensure that required incident response activities take place.

Contents

Introduction

The Economic Development Administration's (EDA's) mission is to lead the federal economic development agenda by promoting innovation and competitiveness, thus preparing American regions for growth and success in the worldwide economy. To fulfill its mission, EDA uses six regional offices[1] to provide services specific to each region's needs.

On December 6, 2011, the U.S. Computer Emergency Response Team (US-CERT)—a part of the Department of Homeland Security (DHS)—notified the Department of Commerce Computer Incident Response Team (DOC CIRT[2]) that it detected a potential malware infection[3] within the Department's systems. DOC CIRT determined the infected components resided within IT systems operating on the Herbert C. Hoover Building (HCHB) network. Accordingly, DOC CIRT informed EDA and the National Oceanic and Atmospheric Administration (NOAA) of a potential infection in their IT systems. NOAA's Computer Incident Response Team analyzed the information provided by DOC CIRT and identified the infected component. NOAA remediated the malware infection and placed the remediated component back into operation by January 12, 2012.

By contrast, on January 24, 2012—believing it had a widespread malware infection—EDA requested the Department isolate its IT systems from the HCHB network. This action resulted in the termination of EDA's operational capabilities for enterprise e-mail and Web site access, and regional office access to database applications and information residing on servers connected to the HCHB network.

Given DOC CIRT's limited incident response capabilities and the perceived extent of the malware infection, the Department and EDA decided to augment the DOC CIRT's incident response team. Additional incident response support was provided by US-CERT, the Department of Energy (DOE) Computer Incident Response Team, the National Institute of Standards and Technology (NIST) Security Implementation and Incident Response Team, and the National Security Agency (NSA). In addition, EDA retained the services of a cybersecurity contractor.

In early February 2012, EDA entered into an agreement with the Census Bureau to provide an interim e-mail capability, Internet access to EDA staff, and Census Bureau surplus laptops for

[1] Regional offices are located in Atlanta, GA; Austin, TX; Chicago, IL; Denver, CO; Philadelphia, PA; and Seattle, WA.

[2] The DOC CIRT provides computer incident response support to most of the Department's operating units that use the Herbert C. Hoover Building network—an Office of the Chief Information Officer-managed infrastructure that many of the bureaus, like EDA, connect to for Department services, Internet connectivity, and communication infrastructure support for internal system operation. Incident response services include interfacing with and reporting incidents to and from the US-CERT, performing malware analysis, interfacing with the Department's network and security operations centers to coordinate changes in network configuration or monitoring resulting from an incident, and providing remediation guidance.

[3] *Malware* is software used by attackers to disrupt computer operation, gather sensitive information, or gain access to computer systems. In EDA's incident, the notification indicated the presence of fake antivirus (FakeAV) software, which deceives a user into executing an application masquerading as antivirus or a malware removal tool.

EDA staff. See appendix B for a detailed timeline of events for EDA's cyber-incident response and recovery.

In accordance with FISMA,[4] we evaluated EDA's incident response and recovery activities in relation to EDA's fiscal year (FY) 2012 cyber incident. We (1) assessed the effectiveness of EDA's IT security program, (2) determined the significant factors that contributed to the incident, and (3) evaluated both completed and planned activities to recover its information systems to support critical operational requirements. See appendix A for details regarding our objectives, scope, and methodology.

[4] The Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C § 3541 (2002), *et seq.*, requires agencies to secure systems through the use of cost-effective management, operational, and technical controls. The statute's goal is to provide adequate security commensurate with the risk and extent of harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency. In addition, FISMA requires inspectors general to evaluate agencies' information security programs and practices by assessing a representative subset of agency systems, and results are reported to the Office of Management and Budget, the Department of Homeland Security, and Congress annually.

Findings and Recommendations

As part of our annual FISMA work, we reviewed EDA's IT security program and the events surrounding its December 2011 cyber incident and recovery efforts. We found that (1) EDA made key incident response and recovery decisions with inaccurate information, (2) DOC CIRT's insufficient incident response efforts degraded the quality of EDA's incident response, and (3) EDA's misdirected efforts hindered the recovery of its IT systems.

I. EDA Based Its Critical Cyber-Incident Response Decisions on Inaccurate Information

EDA believed the incident resulted in a widespread malware infection that was possibly propagating within its systems. Furthermore, EDA believed that its widespread malware infection could spread to other bureaus if its IT systems remained connected to the network, so EDA decided to isolate its IT systems from the HCHB network.

OIG found no evidence to support EDA's beliefs. Specifically, we found no evidence of a widespread malware infection. Further, we found no evidence to support EDA's decision to isolate its IT systems from the HCHB network.

The perception of a widespread malware infection and EDA's incident response decisions are attributable to several factors:

- DOC CIRT's inaccurate analysis and a misunderstanding caused EDA's perception of a widespread malware infection.
- EDA believed that the malware infection would spread to other bureaus on the HCHB network.
- Serious long-standing deficiencies in EDA's IT security program gave credence to EDA's belief that it experienced a widespread malware infection.
- EDA's belief in its widespread malware infection led it to seek validation of a sophisticated cyber attack.[5]
- EDA based its recovery decisions on its belief that it faced a widespread malware infection that included extremely persistent malware.[6]

[5] A *sophisticated cyber attack* typically involves the use of attack techniques, such as exploiting previously unknown vulnerabilities, to successfully compromise a component.

[6] *Extremely persistent malware* cannot be eradicated by reimaging the infected system's hard drive (e.g., malware that infects a device's firmware in order for the infection to persist).

A. *Inaccurate Analysis and a Misunderstanding Caused EDA's Perception of a Widespread Malware Infection*

EDA believed that a cyber attack resulted in an extensive malware infection affecting over half of its components.[7] This belief originated on the first day of incident response activities when DOC CIRT sent EDA inaccurate information concerning the extent of the malware infection, which overstated the number of components involved. Additionally, EDA misunderstood DOC CIRT's follow-up communications, which accurately described the limited extent of the infection. Even though additional communications occurred between DOC CIRT and EDA, each organization continued to have a different understanding of the extent of the malware infection.

DOC CIRT's first incident notification was misleading. On December 6, 2011, US-CERT alerted DOC CIRT to suspicious activity, which involved EDA's systems, on the HCHB network. In an effort to identify infected components, DOC CIRT's incident handler requested network logging information. However, the incident handler unknowingly requested the wrong network logging information (see finding II, subfinding B, for more information on the incident handler). Consequently, on December 7, 2011, DOC CIRT sent an e-mail incident notification to EDA (in response to US-CERT's alert) that inaccurately described the extent of the potential malware infection. Instead of providing EDA a list of potentially infected components, the incident handler mistakenly provided EDA a list of 146 components[8] within its network boundary. Accordingly, EDA believed it faced a substantial malware infection.

DOC CIRT's mistake resulted in a second incident notification. Early on December 8, 2011, an HCHB network staff member informed DOC CIRT that the incident handler's request for network logging information did not identify the infected components. Rather, the response merely identified EDA components residing on a portion of the HCHB network (i.e., the listing of 146 components initially provided to EDA). The HCHB network staff member then performed the appropriate analysis identifying only two components exhibiting the malicious behavior in US-CERT's alert. With this new information, DOC CIRT sent EDA a second e-mail incident notification.

DOC CIRT's second incident notification was vague. DOC CIRT's second incident notification did not clearly explain that the first incident notification was inaccurate. As a result, EDA continued to believe a widespread malware infection was affecting its systems. Specifically, the second incident notification

- *Began by stating the information previously provided about the incident was correct.* EDA interpreted the statement as confirmation of the first incident

[7] EDA's IT system was comprised of approximately 250 IT components (e.g., desktops, laptops, and servers).

[8] The first incident notification contained an attachment with 146 distinct potentially infected components. DOC CIRT, EDA, and external incident responders reported numbers ranging from 142 to 148 components, but the accurate count from the incident notification is 146 components.

notification, when DOC CIRT's incident handler simply meant to confirm EDA was the agency identified in US-CERT's alert. Nowhere in the notification or attachment does the DOC CIRT incident handler identify that there was a mistake or change to the previously provided information.

- *Contained an attachment name that further obscured any clarification.* Although the incident notification's attachment correctly identified only 2 components exhibiting suspicious behavior—not the 146 components that DOC CIRT initially identified—the name of the second incident notification's attachment exactly matched the first incident notification's attachment, obscuring the clarification.

DOC CIRT and EDA's misunderstanding continued. Over the next 5 weeks, additional communications occurred between DOC CIRT and EDA. However, each organization continued to have a different understanding of the extent of the malware infection. DOC CIRT believed the incident affected only two components, whereas EDA believed the incident affected more than half of its components. Several factors contributed to these different interpretations:

- DOC CIRT assumed EDA understood that its second incident notification superseded the first incident notification and that there were only 2 potentially infected components—not 146. However, DOC CIRT did not follow up to establish whether EDA understood the new information.
- EDA responded to the second incident notification by providing a sample of two components (on the list identified in the first incident notification and that were exhibiting malicious behavior) for forensic analysis. DOC CIRT believed the sample to be the same two components identified in the second incident notification.
- When DOC CIRT confirmed that the sample of 2 components was infected with malware, EDA believed that DOC CIRT had confirmed the malware infection for all 146 components listed in the first incident notification.
- DOC CIRT did not retain the first incident notification showing 146 components or document initial incident response activities. Therefore, when DOC CIRT management became involved in the incident response activities, they could not see that a misunderstanding had occurred.

When DOC CIRT asked EDA to carry out typical containment measures (reimaging[9] the infected components), EDA informed DOC CIRT there were too many components involved making typical containment measures unfeasible. DOC CIRT assumed EDA performed an independent analysis to identify additional infected components (even though EDA lacked the necessary capabilities) and assumed EDA was now dealing with a widespread malware infection. Likewise, EDA assumed DOC CIRT was aware of the incident's magnitude, given that DOC CIRT provided the list of

[9] *Reimaging* is the process of reinstalling the operating system and applications on a hard drive, as well as restoring the necessary information from known good backups.

infected components in its first incident notification. Now, EDA and DOC CIRT were operating with the same—albeit inaccurate—belief.

Unfortunately, both organizations continued to propagate the inaccurate information (the basis for the widespread malware infection) during the incident response activities. DOC CIRT's representation of the extent of the malware infection was accepted by DHS and not independently validated in its draft report. DHS's draft report stated, "over 143 systems infected with common fake anti-virus" and "50 percent of EDA's network is infected,"[10] which portrayed a widespread malware infection. The NSA report stated that "the EDA network was extremely inundated with malware" and "the extent of the compromise and the state of the overly infected network will make it very difficult to deconflict the vast amount of indicators."[11] NSA did not independently verify incident information, but it presented similar information to that presented by DHS as fact. As a result, EDA believed these incident reports[12] supported its conclusion regarding the extent of the malware infection.

The misunderstanding went undetected by EDA until December 18, 2012—and by the Department until December 19, 2012—when OIG completed its validation of events and informed both organizations of its initial conclusions.

B. *EDA's Belief That Its Malware Infection Was Spreading Heavily Influenced Its Decision to Isolate Its IT Systems*

On January 24, 2012, EDA, at the recommendation of EDA's current chief information officer (CIO), decided to isolate EDA's IT systems from the HCHB network. EDA's CIO believed that (1) EDA experienced a widespread malware infection, (2) the malware infection was spreading within EDA's IT systems, and (3) the malware infection could spread to other bureaus residing on the HCHB network. Specifically, EDA's CIO believed that an antivirus scan of EDA's primary e-mail server indicated multiple malware infections and the malware infection could propagate to other bureaus on the HCHB network. However, we found no evidence to support these beliefs. Specifically,

- *There was no widespread malware infection.* EDA based its conclusion on inaccurate information (see finding 1, subfinding A).
- *There was no indication of an infection in the e-mail server.* Our analysis of the e-mail server's antivirus logs showed that the antivirus software was up-to-date (e.g., with

[10] U.S. Department of Homeland Security, National Cyber Security Division, February 7, 2012. *Strategic Remediation Strategy for Department of Commerce/Economic Development Administration*, Draft Version 1.0. Washington, DC: DHS National Cyber Security Division, 1. DHS did not issue a final version of its report.

[11] National Security Agency, Computer Network Operations Countermeasures Division, Information Assurance Directorate, May 15, 2012. *IAD Intrusion Response of Department of Commerce Economic Development Administration,* I3331-004R-2012. Ft. Meade, MD: NSA, 4.

[12] NIST did not issue an incident response report. DOE's incident report addressed the results of an assessment on one component—analysis indicated trace evidence of an attempted infection but no extremely persistent malware—not the incident as a whole.

the most current software version and latest malware definitions), was scanning weekly, and had not identified any malware. Not only was EDA's CIO unable to substantiate his assertion with credible evidence, EDA's IT staff did not support the assertion of an infection in the e-mail server.

- *The e-mail server did not pose an increased risk.* EDA's outbound e-mail traffic does not pass through any other e-mail systems before reaching the Internet; therefore, the infection would not have spread the way EDA's CIO believed. Further, e-mail traffic in general does not pose a risk to an e-mail server, as infected e-mail attachments typically require user interaction. Additionally, the Department has security measures to address infected e-mail attachments. Thus, EDA's e-mail server did not pose an increased risk, even if it had been infected.

C. *EDA's Severely Deficient IT Security Program Gave Credibility to the Purported Widespread Malware Infection*

Since 2006, OIG has identified significant deficiencies in EDA's IT security program. NSA's 2009 review[13] further emphasized these deficiencies with the discovery of multiple common malware[14] infections. We reviewed EDA's IT security program after its incident and found that many of the deficiencies identified in past reviews remained unremediated for more than 4 years (see table 1 below for examples of deficient security measures).

[13] In 2009, NSA reviewed security measure implementations on IT systems operating on the HCHB network.

[14] *Common malware* (e.g., spyware, virus, or Trojans), although typically malicious and potentially harmful, can be removed using common cleaning tools and processes (e.g., reimaging).

Table 1. Examples of EDA's Long-Standing Security Deficiencies

Security Measure	Definition	Significance	Deficiencies Identified In OIG and NSA Reviews[a]
Secure Configurations	The processes an organization uses to define how to secure its IT products (e.g., operating systems, databases, and web applications)—limiting the functions of a component to minimal operations	Without effective secure configurations, an organization will not effectively limit unauthorized use of its components. Securely configuring IT products is a fundamental and critical security measure (one of DHS's and NSA's key recovery recommendations to EDA).	2006, 2009, 2010, 2012: EDA had not defined or implemented this security measure.
Patch Management	The processes an organization uses to track and correct software (e.g., operating system and application) vulnerabilities	Without effective patch management, vulnerabilities can remain unremediated, leaving components vulnerable to compromise and information less secure.	2009, 2010, 2012: EDA did not reliably track[b] or correct vulnerabilities (some for many years).
Auditing and Monitoring	The processes and tools used to detect the use of systems and information by an unauthorized user or external attackers	Without effective auditing and monitoring, an organization may not be able to track unauthorized access to components and information, follow an attacker's activities, or reconstruct what happened when an incident occurs.	2006, 2012: EDA did not monitor for suspicious activity in its systems.
Security Assessments	Assessments performed to determine the extent of security mechanism implementation	Without the appropriate assessment of security mechanisms, organizations will not have an accurate picture of the risks to the system and management will not have the information necessary to make appropriate risk-based decisions.	2006, 2010, 2012: EDA's assessment methodologies did not appropriately identify deficiencies or convey risks to operations and information.

Source: OIG FISMA reviews from 2006, 2010, and 2012 and NSA's 2009 review

[a] Not all security mechanisms were assessed in the course of each OIG FISMA review or in NSA's 2009 review.

[b] Prior to May 2011, EDA's systems had not been scanned for almost a year. When scans resumed, they identified over 35,000 potential vulnerabilities. Scans performed in December 2011, just prior to the incident, indicated that EDA was struggling to remediate these vulnerabilities. OIG's post-incident review found 37 percent (56 of 151) of the vulnerabilities highlighted by the NSA in 2009 still exist—the NSA asserted in its incident response report that EDA did not address remediation recommendations from the NSA's 2009 assessment of EDA's IT systems.

EDA's current CIO joined the organization in April 2011. The CIO inherited an IT security program suffering from longstanding and significant security deficiencies. For example, the CIO briefed EDA leadership that (1) EDA IT staff lacked appropriate IT security skills, (2) system configuration management and secure configurations were not implemented, and (3) systems were not appropriately monitored.

The Department and EDA[15] knew of EDA's many IT security program deficiencies; therefore, they more readily believed there was a widespread malware infection. Further, when external incident responders analyzed the incident, they too observed pervasive deficiencies—the result of too few implemented IT security mechanisms. Their observations further reinforced the credibility of a widespread malware infection. Furthermore, the pervasive deficiencies led the Office of the Chief Information Officer (OCIO) and EDA not to question the accuracy of the extent of the malware infection, despite a lack of supporting evidence.

D. *EDA Sought Validation of a Sophisticated Cyber Attack*

EDA hired a cybersecurity contractor—in addition to other external agencies already responding to the incident—to perform an in-depth evaluation of the malware infection in its systems. EDA's CIO and senior leadership were specifically concerned about nation-state actors[16] and the presence of extremely persistent malware that would prohibit typical containment measures, such as reimaging infected components for immediate use.

On January 30, 2012, EDA's cybersecurity contractor began looking for suspicious activity and malware infections. Preliminary analysis found indications of extremely persistent malware and suspicious activity on EDA's components. EDA immediately acted upon this preliminary information and began an investigation of its entire IT component inventory for potential infections.

E. *External Incident Responders Found No Evidence of a Widespread Malware Infection or Extremely Persistent Malware*

Within 2 weeks of beginning its incident response activities, EDA's cybersecurity contractor found the initial indications of extremely persistent malware were false positives—not actual malware infections. However, EDA's CIO sought guaranteed assurance that the components were infection-free and no malware could persist. External incident responders were unable to provide the assurance EDA's CIO sought, because doing so involved proving that an infection *could not* exist rather than that one *did not* exist. By April 16, 2012, despite months of searching, EDA's cybersecurity contractor was unable to find any extremely persistent malware or indications of a targeted attack on EDA's systems. Further, the NSA and US-CERT did not find nation-state activity or extremely persistent malware.

On May 15, 2012, EDA's management determined that the forensics investigation was unlikely to yield new evidence and instead focused on cleaning its data[17] and other

[15] The Department's annual internal IT reviews have identified IT security deficiencies in EDA's IT security program.

[16] *Nation-state actors* are hackers acting on behalf of a nation's government to engage in nefarious activity, such as cyber war and theft of intellectual property.

[17] *Cleaning* involves using several antivirus products to scan data files for indications of an infection.

recovery activities. Ultimately, incident responders identified only six components[18] with malware infections. These malware infections could have been remediated using typical containment measures (e.g., reimaging), which normally have a minimal operational impact. Additionally, EDA's cybersecurity contractor's data cleaning efforts did not identify any additional components with a malware infection (the contractor did identify the existence of common malware contained in archived e-mail attachments and temporary Internet browser files[19]). Typically, antivirus software prevents common malware from executing; as a result, the contractor did not consider the malware a threat to EDA's components.

Given EDA's history of common malware infections (the NSA identified common malware on EDA's IT systems in its 2009 review), there was a high probability that external incident responders would find some malware infections when investigating EDA's incident. In fact, EDA's lack of implemented IT security and the significant number of easily exploitable vulnerabilities negated an attacker's need to use costly attack techniques (sophisticated cyber attacks) to compromise EDA's systems. EDA's deficient IT security posture made it likely that external incident responders would find common malware. In the end, nothing identified on EDA's components posed a significant risk to EDA's operations.

However, EDA's CIO concluded that the risk, or potential risk, of extremely persistent malware and nation-state activity (which did not exist) was great enough to necessitate the physical destruction of all of EDA's IT components.[20] EDA's management agreed with this risk assessment and EDA initially destroyed more than $170,000 worth of its IT components,[21] including desktops, printers, TVs, cameras, computer mice, and keyboards. By August 1, 2012, EDA had exhausted funds for this effort and therefore halted the destruction of its remaining IT components, valued at over $3 million. EDA intended to resume this activity once funds were available. However, the destruction of IT components was clearly unnecessary because only common malware was present on EDA's IT systems.

Conclusion

Since EDA did not validate the information (e.g., number of infected components and potentially spreading malware infection) it used to make its key decisions, it unnecessarily expended a large portion of its IT budget and many months investigating its incident and planning for the recovery of its IT systems. Despite only finding common malware

[18] External incident responders identified six infected components, two with rootkits (software that enables a persistent infection) and four with common malware—including the two components DOC CIRT identified.

[19] Web browsers store on the IT component's hard drive the information downloaded from each Web page visited to enhance browser performance. Although the industry labels this information "temporary," the information remains on the component's hard drive until manually deleted.

[20] Prior to the incident, EDA purchased laptops intended as replacements for its current desktop and laptop environment. Because these new laptops had not been operational, EDA could incorporate them into its new IT systems.

[21] EDA tracks the acquisition value, rather than the depreciated value, of its components.

infections, EDA's management and CIO remained convinced that there *could be* extremely persistent malware somewhere in EDA's IT systems.

To recover from its perceived widespread malware infection, EDA took the following significant recovery steps:

- Employed a cybersecurity contractor to investigate the malware infection and ensure its important data was free of malware
- Entered into an agreement with the Census Bureau to provide EDA with an interim, minimalistic IT solution[22]
- Physically destroyed IT components to ensure that a potential infection could not persist
- Employed a contractor to assist in the development of a long-term recovery solution

EDA expended more than $2.7 million—over half of EDA's FY 2012 IT budget (see table 2 below for expenditures and finding 3 for further discussion of recovery activities) in pursuit of these recovery activities. EDA's persistent mistaken beliefs resulted in an excessive response and ultimately unnecessary expenditure of valuable resources.

Table 2. Significant Recovery Activity Expenditures

Activity	Expenditure[a]
Cybersecurity contractor investigation of malware infection and data cleaning	$823,000
Temporary infrastructure, pending long-term IT solution	$1,061,000
Destruction of IT equipment[b]	$175,000
Contractor assistance for a long-term recovery solution	$688,000
TOTAL EXPENDITURES	**$2,747,000**

Source: Contracts from EDA's recovery efforts

[a] All values in the table are rounded.

[b] EDA paid $4,300 to destroy $170,500 in IT equipment—these are rounded values.

II. Deficiencies in the Department's Incident Response Program Impeded EDA's Incident Response

Deficiencies in HCHB's incident response program (DOC CIRT) significantly contributed to EDA's inaccurate belief that it experienced a widespread malware infection; consequently, DOC CIRT and EDA propagated inaccurate information that went unidentified for months after EDA's incident.

We found the following deficiencies in DOC CIRT's incident response activities:

[22] EDA did not intend for the Census Bureau to provide a final IT recovery solution. Instead, the Census Bureau provided an interim solution that met EDA's minimum operating requirements until EDA could develop a permanent solution.

- DOC CIRT's incident handlers did not follow the Department's incident response procedures.
- DOC CIRT's incident handler for EDA's incident did not have the requisite experience or qualifications.[23]
- DOC CIRT did not adequately coordinate incident response activities.

A. DOC CIRT Did Not Follow Incident Response Procedures

When responding to EDA's incident, DOC CIRT staff did not appropriately follow incident response procedures. Specifically, DOC CIRT staff did not (1) properly document the initial incident response activities, (2) establish the extent of the malware infection, and (3) perform a required containment procedure.

DOC CIRT did not properly document the initial incident response activities. We found DOC CIRT did not document its communications with EDA or record pertinent incident details like requests, actions taken, or analysis results. For example, the incident handler deleted the first incident notification showing 146 potentially infected components and retained only the second incident notification showing 2 potentially infected components. Had the incident handler documented all information, per the Department's incident response procedures, it would have been more likely that other DOC CIRT staff or external incident responders could have identified the misunderstanding regarding the extent of the malware infection. As a result, EDA, the Department, and external incident responders would not have needed to expend resources to resolve a widespread malware infection that did not exist.

DOC CIRT did not accurately establish the extent of the malware infection. We found that DOC CIRT staff did not appropriately establish the extent of the malware infection prior to proceeding with other incident response activities (e.g., conducting forensic analysis). The Department's incident response procedures require that incident handlers establish the extent of an infection before proceeding with other incident response activities so that all involved in the incident response efforts can formulate realistic containment and mitigation strategies. Since DOC CIRT did not accurately establish the extent of EDA's incident, EDA's misunderstanding (e.g., EDA thought there were 146 infected components instead of only 2) influenced everyone's perception of the incident and contributed to EDA's unnecessary recovery and remediation activities.

DOC CIRT did not appropriately perform a required containment procedure. When HCHB network staff correctly determined that US-CERT's alert involved two components, DOC CIRT's incident handler should have followed the Department's required containment procedure. Specifically, the incident handler should have

[23] The Space and Naval Warfare Systems Command (SPAWAR), a Department of the Navy organization, provided the OCIO cybersecurity technical support—including an incident handler—specified in an interagency agreement that ended on February 8, 2012.

directed HCHB security operations center staff to block HCHB network activity associated with the malicious address identified in US-CERT's alert. Furthermore, on December 15, 2011, EDA reminded DOC CIRT's incident handler to block the malicious address. However, DOC CIRT did not initiate this action until January 24, 2012, the same day EDA's systems were isolated from the HCHB network.

B. *DOC CIRT's Inexperienced Staff Hindered EDA's Incident Response*

DOC CIRT's inexperienced staff and inadequate knowledge of EDA's incident response capabilities[24] hindered its ability to provide adequate incident response services. DOC CIRT's incident handler managing EDA's initial incident response activities had minimal incident response experience, no incident response training, and did not have adequate skills to provide incident response services. The lack of experience, training, and skills led the incident handler to request the wrong network logging information (i.e., perform the wrong incident analysis), which led EDA to believe it had a widespread malware infection, and deviate from mandatory incident response procedures. The Department's Office of the Chief Information Officer should have ensured that all DOC CIRT staff met the Department's minimum incident response qualifications.

In addition, DOC CIRT staff did not understand that there was a preexisting expectation of specific incident response services, as outlined in the service level agreement (SLA) between the DOC CIRT and EDA. This agreement clearly states DOC CIRT's obligated incident response services (e.g., investigation, forensics, and reverse engineering) and defines EDA's incident response responsibilities (e.g., reporting incidents and dealing with quarantined or deleted malware). Since DOC CIRT staff did not understand this agreement, they inaccurately assumed EDA was capable of performing its own incident analysis activities (e.g., determining the extent of the malware infection).

C. *DOC CIRT Did Not Adequately Coordinate EDA's Incident Response Activities*

DOC CIRT is responsible for coordinating incident response efforts (e.g., dissemination of information and coordination of incident response activities). However, DOC CIRT did not effectively coordinate EDA's incident response activities. The inadequate coordination resulted in haphazard communications, in which external incident responders received minimal direction. As a result,

- *External incident responders performed redundant forensics analysis on the same components*. External incident responders unnecessarily and wastefully expended resources to develop the same conclusions.
- *The quality of EDA's incident response suffered.* DOC CIRT and EDA did not use external incident responders' technical knowledge and experience to their fullest potential.

[24] Each Departmental bureau has designated incident responders and its own set of internal incident response capabilities. The skill level (as gauged by an incident responder's training, certifications, and previous incident response experience) and the tools available within each bureau differ.

- *Gaining a full understanding of EDA's incident was difficult.* Inadequate coordination resulted in undirected incident response efforts and uncoordinated distribution of pertinent incident information, making it difficult to gain a holistic and unbiased view of the incident.

Conclusion

OIG briefed the Department's CIO on weaknesses within the DOC CIRT that we identified during our review of incident response activities. Accordingly, the Department has taken actions to correct DOC CIRT's weaknesses. Specifically, the Department is taking steps to:

- Ensure staff receive appropriate training
- Update incident response procedures
- Review services offered (including the needs and capabilities of each bureau)
- Develop agreements with external agencies to provide incident response expertise
- Hire experienced incident handlers

III. Misdirected Efforts Hindered EDA's IT System Recovery

Based on EDA's erroneous belief that it had a widespread malware infection, and its incorrect interpretation of recovery recommendations, EDA focused its recovery efforts on replacing its IT infrastructure and redesigning its business applications. EDA should have concentrated its resources on quickly and fully recovering its IT systems (e.g., critical business applications) to ensure its operational capabilities.

Our review of EDA's recovery activities found the following:

- EDA decided to replace its entire IT infrastructure based on its incorrect interpretation of recovery recommendations.

- EDA's recovery efforts were unnecessary.

A. EDA Acted on Its Incorrect Interpretation of Recovery Recommendations

EDA received similar recovery recommendations from NSA and DHS that focused on quickly recovering IT services (e.g., reimaging infected components), implementing security mechanisms and best practices, and monitoring its recovered IT systems for suspicious activity. These recovery recommendations, conventional practices used to recover from a cyber incident, were appropriate for EDA's recovery.

EDA's continued belief in the necessity of permanent remediation actions (i.e., destroying its IT components) and a significant malware infection contributed to EDA incorrectly interpreting the recovery recommendations. EDA erroneously interpreted one of DHS's draft recommendations—"a complete network rebuild is recommended"—as both prescriptive guidance and direct support for its decision to replace its entire IT infrastructure. However, DHS's full draft recommendation advised EDA to reimage all IT components and implement required security measures, effectively rebuilding its network. Neither DHS's nor NSA's recommendations provided a basis for EDA's decisions to replace its IT infrastructure and destroy its IT components.

B. *EDA's Recovery Efforts Were Unnecessary*

Despite recovery recommendations from DHS and NSA advising EDA to focus on quickly and fully recovering its IT systems, EDA focused instead on building a new, improved IT infrastructure and redesigning its business applications. In September 2012 (8 months after isolation), EDA leadership presented to the Commerce IT Review Board (CITRB) a request to reprogram funds to carry out its recovery efforts; the CITRB did not approve EDA's request.[25] EDA estimated it would need over $26 million disbursed in the next 3 years (an increase from $3.6 million to approximately $8.83 million, or about 2.5 times more, to the bureau's average annual IT budget) to fund its recovery efforts. However, EDA's intended recovery efforts

- *Had a fundamental flaw in acquiring funding.* EDA leadership did not understand that the funds it requested to reprogram—over $17 million originally designated for public works and disaster recovery—would actually need to be "repurposed."[26]
- *Had an unrealistic time frame for acquiring requested funding.* The request's time frame would have required EDA to gain approval by October 2012 in order to maintain the intended schedule. This was an extremely aggressive time frame, given the process (in which CITRB approval was the first step) and time necessary to attain proper clearance to use the funds.
- *Would leave EDA reliant on a less effective grants management process.* EDA users would only have limited access to critical business applications. EDA was not scheduled to complete development of replacement applications until the end of FY 2014 (more than 2 years after isolation).
- *Conflicted with the Department's ongoing development of a grants management shared service.* EDA's request for funding to redesign its business applications overlapped with the Department's development of a grants management shared service.

Further, the following contradicted the direction of EDA's recovery efforts:

[25] The CITRB provides oversight, review, and advice to the Secretary and Deputy Secretary on both IT and non-IT investments that meet certain criteria. This advice includes recommendations for approval or disapproval of funding for new systems and investments, as well as major modifications to existing systems and investments.

[26] According to EDA, it would have needed Departmental and OMB approval of its request to fund its recovery efforts before presenting the request to Congress. EDA would also have needed to request that Congress change the law dictating the original purpose and use of the funds requested.

- External incident responders identified only common malware that could be easily mitigated. As a result, there was no need for EDA to destroy or replace existing IT components.
- NSA found no malware infection in the servers hosting EDA's primary business application. Additionally, there was no evidence to suggest that EDA's primary business application had been targeted by a cyber attack or maliciously altered—thus, EDA could have put the application back into full operation.

Conclusion

Although EDA intended to use federal government shared services or outsourced commercial services during its recovery efforts, EDA had not finalized a recovery solution. Further, the Department had existing shared IT services (e.g., image for rebuilding infected components, enterprise e-mail, and help desk services) that were readily available to EDA. However, only after OIG informed the Department and EDA that there was no widespread malware infection, and therefore no significant incident, did the Department and EDA enact a swift recovery of EDA's IT systems using the Department's shared services.

Once it started recovery efforts in February 2013, the Department needed only a little longer than 5 weeks to restore EDA's former operational capabilities.[27] By comparison, EDA's incomplete efforts spanned almost a year. Specifically, the Department provided EDA with enterprise e-mail, account management services, help desk support services, and a securely configured and uniform image for its laptops. Additionally, the Department restored EDA users' access to critical business applications.

For the time being, EDA will retain responsibility for maintaining its business applications; however, it may in the future use the Department's grants management services. With the Department developing and maintaining the IT systems, there is a greater likelihood that the Department will appropriately implement the required security measures (e.g., secure configurations, auditing and monitoring, and patch management) that EDA struggled to implement. Fortunately, for EDA, its involvement in the Department's shared services initiatives not only restored its critical IT systems and business applications, but should also reduce its IT budgetary requirements.

[27] EDA's previous access to NOAA's financial system has yet to be restored.

Recommendations

We recommend that the Deputy Assistant Secretary for EDA:

1. Identify EDA's areas of IT responsibility and ensure the implementation of required security measures.
2. Determine whether EDA can reduce its IT budget and staff expenditures, through the increased efficiencies of EDA's involvement in the Department's shared services.
3. Ensure that EDA does not destroy additional IT inventory that was taken out of service as a result of this cyber incident.

We recommend that the Department's Chief Information Officer:

1. Ensure DOC CIRT can appropriately and effectively respond to future cyber incidents.
2. Ensure incident response procedures clearly define DOC CIRT as the incident response coordinator for the bureaus relying on DOC CIRT's incident response services.
3. Ensure that DOC CIRT management has proper oversight and involvement in cyber incidents to ensure that required incident response activities take place.

Summary of Agency and Departmental Responses and OIG Comments

The Deputy Assistant Secretary of Commerce for Economic Development and the Department's Chief Information Officer (CIO) provided written responses to a draft of this report (see appendixes C and D). We provide summaries of these responses and our comments below.

EDA Response

The Deputy Assistant Secretary of Commerce for Economic Development concurred with our recommendations and noted that EDA has begun implementation of the recommendations.

EDA also noted that (1) EDA's focus has been to fully and efficiently recover its IT systems, (2) it has been abundantly cautious in its efforts to protect its staff, other Department systems, grantees, clients, and other federal partners, (3) it continued to conduct and complete its important work on time despite the interruption, and (4) it worked closely with the Census Bureau for an interim recovery solution and, more recently, leveraged the Department's shared services. EDA's response identified corrective actions it has taken and plans to take to implement our recommendations.

EDA stated in its response that it "appreciates the Office of Inspector General's (OIG) comprehensive review and continued involvement from the very early days of the incident when EDA proactively requested OIG's review of the matter." While we initiated this audit at the request of the former Acting Deputy Secretary of Commerce, we appreciate EDA's cooperation throughout our audit.

In its response, EDA noted that its long-term recovery plan already included greater use of shared services by leveraging Department-wide IT assets. However, prior to our briefing on December 18, 2012, EDA had not finalized a recovery solution, such as using the Department's available shared services.

Department CIO Response

The Department's CIO concurred with our recommendations related to DOC CIRT, noting that the Department has initiated a comprehensive incident response improvement project. The CIO further stated that the following project milestones have already been completed: (1) conducting a third-party assessment of the DOC CIRT policies, procedures, and capabilities; (2) hiring experienced and certified incident handlers; and (3) implementing an improved incident tracking system.

In addition, the Department's CIO stated that, within the past 6 months, the OCIO and the Office of the Secretary (OS) IT Operations worked closely with EDA to restore its functionality by bringing EDA's grants management system online and bringing EDA's office automation and IT service desk under the OS Information Technology Services.

Appendix A: Objectives, Scope, and Methodology

Our objective was to evaluate EDA's information security program and its recovery activities in relation to EDA's cyber incident. We (1) assessed the effectiveness of EDA's IT security program, (2) determined the significant factors that contributed to the incident, and (3) evaluated both completed and planned activities to recover its information systems to support critical operational requirements. To do so, we

- Reviewed system-related artifacts, including policy and procedures, planning documents, and other material supporting the security authorization process
- Reviewed artifacts related to EDA's incident, including incident reports, forensic analysis, logs, written communications, and other incident documentation
- Interviewed operating unit and Department OCIO personnel, including system owners, IT security officers, IT administrators, external incident responders, and organizational directors and administrators regarding the security and operation of EDA's IT systems and the incident

We also reviewed EDA's compliance with the following applicable provisions of law, regulations, and mandatory guidance:

- The Federal Information Security Management Act of 2002
- Information Technology Security Program Policy, U.S. Department of Commerce, introduced by the Chief Information Officer on March 9, 2009, and applicable Commerce Information Technology Requirements
- NIST Federal Information Processing Standards Publications
    - 199, Standards for Security Categorization of Federal Information and Information Systems
    - 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST Special Publications
    - 800-34, Contingency Planning Guide for Federal Information Systems
    - 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems
    - 800-53, Recommended Security Controls for Federal Information Systems and Organizations

- 800-53A, Guide for Assessing the Security Controls in Federal Information Systems
- 800-61, Computer Incident Handling Guide
- 800-70, Security Configuration Checklists Program for IT Products

We conducted our fieldwork from June 2012 to February 2013. We performed this audit under the authority of the Inspector General Act of 1978, as amended, and Department Organization Order 10-13, and in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

Appendix B: Detailed Timeline of EDA's Cyber Incident Response and Recovery

Cyber Incident

12/6/2011 US-CERT notifies DOC CIRT of a cyber incident (components communicating with fake antivirus sites).

12/7/2011 DOC CIRT sends EDA a first incident notification concerning US-CERT's alert. The notification contains an inaccurate list of 146 potentially infected components.

12/8/2011 DOC CIRT sends EDA a second incident notification containing completed analysis that identified only two infected components.

12/9/2011 EDA's ITSO informs EDA's CIO that EDA experienced a potential widespread malware infection.

12/13/2011 EDA's ITSO requests forensic assistance from DOC CIRT and on 12/14/2011 EDA provided DOC CIRT with the hard drives from two components that were exhibiting malicious behavior.

12/15/2011 EDA asks DOC CIRT to block the malicious sites and addresses associated with the US-CERT alert.

12/16/2011 EDA's CIO informs EDA's leadership that the malware infection is potentially widespread.

1/18/2012 DOC CIRT notifies EDA that it identified a common malware infection on the two components EDA provided to DOC CIRT on 12/14/2011. DOC CIRT advises EDA to reimage the infected drives and put the remediated components back into operation. EDA informs DOC CIRT that it cannot do this because there are too many infected components.

1/20/2012 EDA's CIO notifies EDA's user base of the malware infection and advises that all users follow good security practices. DOC CIRT requests US-CERT's assistance and US-CERT arrives onsite.

1/24/2012 EDA's CIO believes that the e-mail server experienced a complete operational failure and, upon restoration, an antivirus scan showed multiple malware infections. EDA's CIO informed EDA's leadership (and the Department's Deputy CIO) of the need to isolate EDA from the HCHB network. EDA takes the following actions: disables its Microsoft Exchange e-mail server connection; disables Internet access; disables its connection with regional offices; and maintains local file-share service availability.

1/27/2012 DOE and NIST incident responders assist onsite with the incident response.

1/30/2012 EDA hires a cyber security contractor to assist at the EDA CIO's discretion. US-CERT issues a preliminary analysis report, which indicates the presence of common malware but no nation-state activity or extremely persistent malware.

2/2/2012 The Department requests NSA's assistance to investigate the malware infection.

2/3/2012 DOE releases its report detailing assessment results from an assessment of one component that indicated a common malware infection, but did not identify any nation-state activity or extremely persistent malware.

2/7/2012 DHS issues a report that summarizes its findings and includes recommendations for remediating the infection and establishing good IT security practices. Additionally, the report used inaccurate information provided by DOC CIRT to portray EDA's incident as widespread.

2/14/2012 NSA assists onsite with incident response activities.

2/17/2012 NSA analysis of the Linux systems finds no evidence of an intrusion or malware infection.

5/15/2012 NSA releases a report stating that EDA had a widespread common malware infection. NSA portrayed this information as fact, even though it did not independently validate the information it received from DHS. However, NSA did analyze EDA's Linux servers and found that the servers were not infected and there was no indication of nation-state activity or extremely persistent malware.

Recovery

1/24/2012 EDA operates its existing IT infrastructure in isolation during interim recovery activities in order to meet its deadlines for grants management.

2/6/2012 EDA begins coordination with the Census Bureau on its interim recovery activities.

2/14/2012 EDA establishes a Web presence and makes e-mail service available to a limited number of Blackberry users.

3/25/2012 The Census Bureau restores Blackberry service for all EDA staff and EDA completes the distribution of laptops to all users. This provides office automation capabilities, e-mail services, and Internet access for all users.

4/5/2012 EDA provides users access to a stand-alone implementation of its business applications, which contains historical data necessary to complete its mission activities.

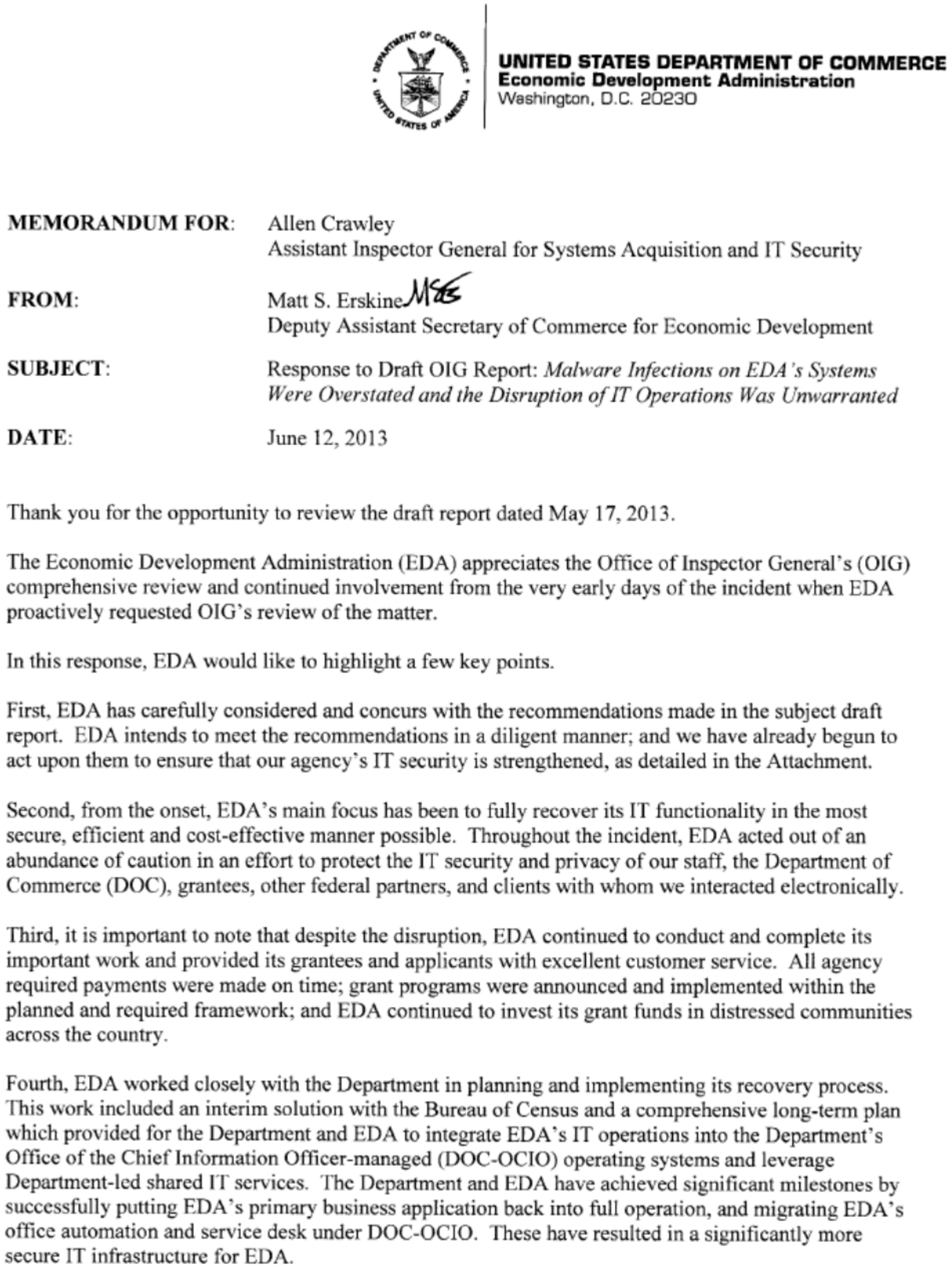
5/15/2012 EDA stops its forensic analysis activities and switches to full-time data cleaning, involving the use of several antivirus products to scan data files for indications of an infection. The cybersecurity contractor did not identify any additional components with a malware infection (the contractor did identify the existence of common malware contained in archived e-mail attachments and temporary Internet browser files).

9/5/2012 EDA presents a request to the Commerce IT Review Board (CITRB) for funding to carry out its recovery efforts. The CITRB does not approve EDA's request, necessitating changes to the intended recovery efforts.

2/6/2013 OCIO begins restoration of EDA's IT systems.

3/15/2013 OCIO restores EDA's IT operations, including restoring access for all users to its critical grants management applications.

Appendix C: Agency Response



UNITED STATES DEPARTMENT OF COMMERCE
Economic Development Administration
Washington, D.C. 20230

MEMORANDUM FOR: Allen Crawley
Assistant Inspector General for Systems Acquisition and IT Security

FROM: Matt S. Erskine
Deputy Assistant Secretary of Commerce for Economic Development

SUBJECT: Response to Draft OIG Report: *Malware Infections on EDA's Systems Were Overstated and the Disruption of IT Operations Was Unwarranted*

DATE: June 12, 2013

Thank you for the opportunity to review the draft report dated May 17, 2013.

The Economic Development Administration (EDA) appreciates the Office of Inspector General's (OIG) comprehensive review and continued involvement from the very early days of the incident when EDA proactively requested OIG's review of the matter.

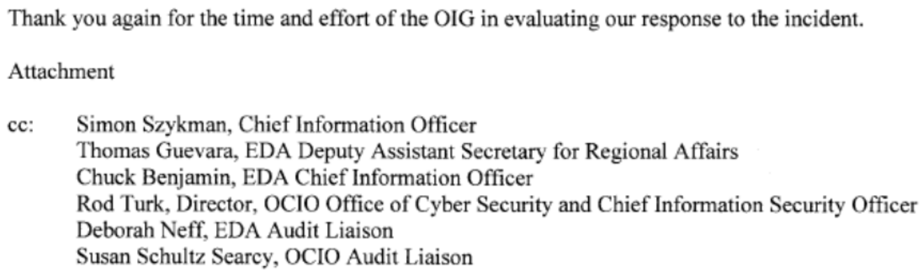
In this response, EDA would like to highlight a few key points.

First, EDA has carefully considered and concurs with the recommendations made in the subject draft report. EDA intends to meet the recommendations in a diligent manner; and we have already begun to act upon them to ensure that our agency's IT security is strengthened, as detailed in the Attachment.

Second, from the onset, EDA's main focus has been to fully recover its IT functionality in the most secure, efficient and cost-effective manner possible. Throughout the incident, EDA acted out of an abundance of caution in an effort to protect the IT security and privacy of our staff, the Department of Commerce (DOC), grantees, other federal partners, and clients with whom we interacted electronically.

Third, it is important to note that despite the disruption, EDA continued to conduct and complete its important work and provided its grantees and applicants with excellent customer service. All agency required payments were made on time; grant programs were announced and implemented within the planned and required framework; and EDA continued to invest its grant funds in distressed communities across the country.

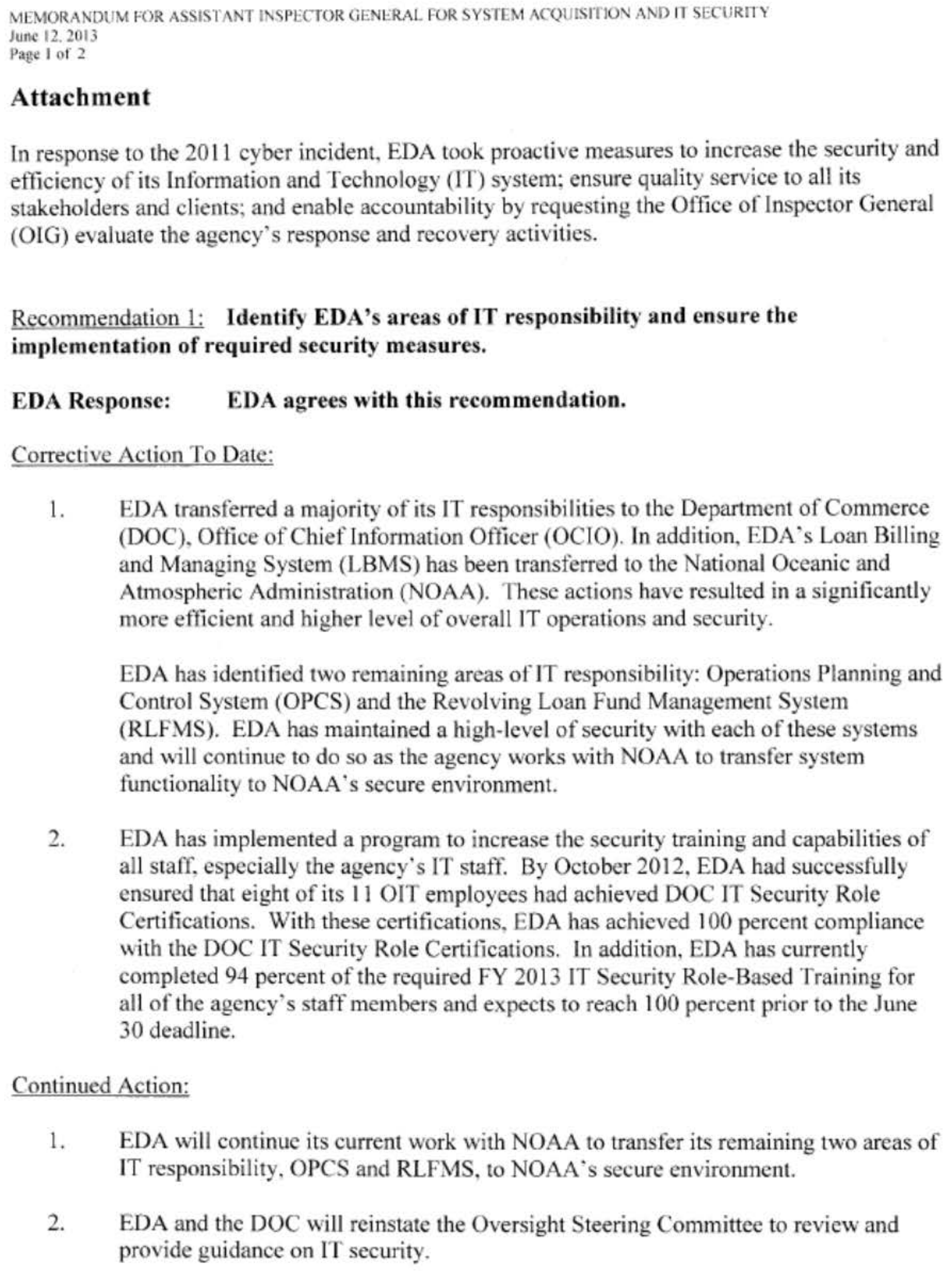
Fourth, EDA worked closely with the Department in planning and implementing its recovery process. This work included an interim solution with the Bureau of Census and a comprehensive long-term plan which provided for the Department and EDA to integrate EDA's IT operations into the Department's Office of the Chief Information Officer-managed (DOC-OCIO) operating systems and leverage Department-led shared IT services. The Department and EDA have achieved significant milestones by successfully putting EDA's primary business application back into full operation, and migrating EDA's office automation and service desk under DOC-OCIO. These have resulted in a significantly more secure IT infrastructure for EDA.



Thank you again for the time and effort of the OIG in evaluating our response to the incident.

Attachment

cc: Simon Szykman, Chief Information Officer
Thomas Guevara, EDA Deputy Assistant Secretary for Regional Affairs
Chuck Benjamin, EDA Chief Information Officer
Rod Turk, Director, OCIO Office of Cyber Security and Chief Information Security Officer
Deborah Neff, EDA Audit Liaison
Susan Schultz Searcy, OCIO Audit Liaison



MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR SYSTEM ACQUISITION AND IT SECURITY
June 12, 2013
Page 1 of 2

Attachment

In response to the 2011 cyber incident, EDA took proactive measures to increase the security and efficiency of its Information and Technology (IT) system; ensure quality service to all its stakeholders and clients; and enable accountability by requesting the Office of Inspector General (OIG) evaluate the agency's response and recovery activities.

Recommendation 1: **Identify EDA's areas of IT responsibility and ensure the implementation of required security measures.**

EDA Response: EDA agrees with this recommendation.

Corrective Action To Date:

1. EDA transferred a majority of its IT responsibilities to the Department of Commerce (DOC), Office of Chief Information Officer (OCIO). In addition, EDA's Loan Billing and Managing System (LBMS) has been transferred to the National Oceanic and Atmospheric Administration (NOAA). These actions have resulted in a significantly more efficient and higher level of overall IT operations and security.

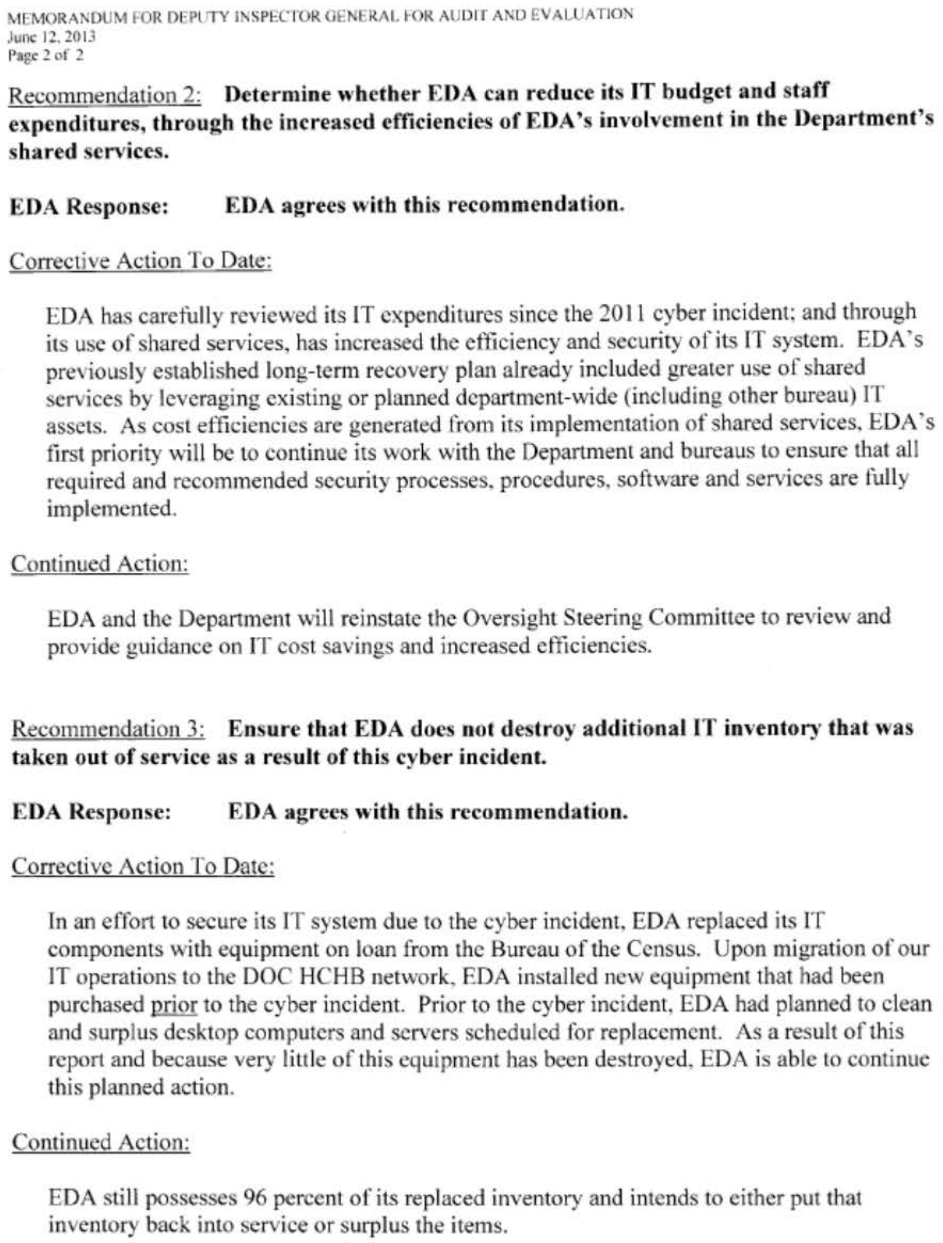
   EDA has identified two remaining areas of IT responsibility: Operations Planning and Control System (OPCS) and the Revolving Loan Fund Management System (RLFMS). EDA has maintained a high-level of security with each of these systems and will continue to do so as the agency works with NOAA to transfer system functionality to NOAA's secure environment.

2. EDA has implemented a program to increase the security training and capabilities of all staff, especially the agency's IT staff. By October 2012, EDA had successfully ensured that eight of its 11 OIT employees had achieved DOC IT Security Role Certifications. With these certifications, EDA has achieved 100 percent compliance with the DOC IT Security Role Certifications. In addition, EDA has currently completed 94 percent of the required FY 2013 IT Security Role-Based Training for all of the agency's staff members and expects to reach 100 percent prior to the June 30 deadline.

Continued Action:

1. EDA will continue its current work with NOAA to transfer its remaining two areas of IT responsibility, OPCS and RLFMS, to NOAA's secure environment.

2. EDA and the DOC will reinstate the Oversight Steering Committee to review and provide guidance on IT security.



MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT AND EVALUATION
June 12, 2013
Page 2 of 2

Recommendation 2: **Determine whether EDA can reduce its IT budget and staff expenditures, through the increased efficiencies of EDA's involvement in the Department's shared services.**

EDA Response: EDA agrees with this recommendation.

Corrective Action To Date:

EDA has carefully reviewed its IT expenditures since the 2011 cyber incident; and through its use of shared services, has increased the efficiency and security of its IT system. EDA's previously established long-term recovery plan already included greater use of shared services by leveraging existing or planned department-wide (including other bureau) IT assets. As cost efficiencies are generated from its implementation of shared services, EDA's first priority will be to continue its work with the Department and bureaus to ensure that all required and recommended security processes, procedures, software and services are fully implemented.

Continued Action:

EDA and the Department will reinstate the Oversight Steering Committee to review and provide guidance on IT cost savings and increased efficiencies.

Recommendation 3: **Ensure that EDA does not destroy additional IT inventory that was taken out of service as a result of this cyber incident.**

EDA Response: EDA agrees with this recommendation.

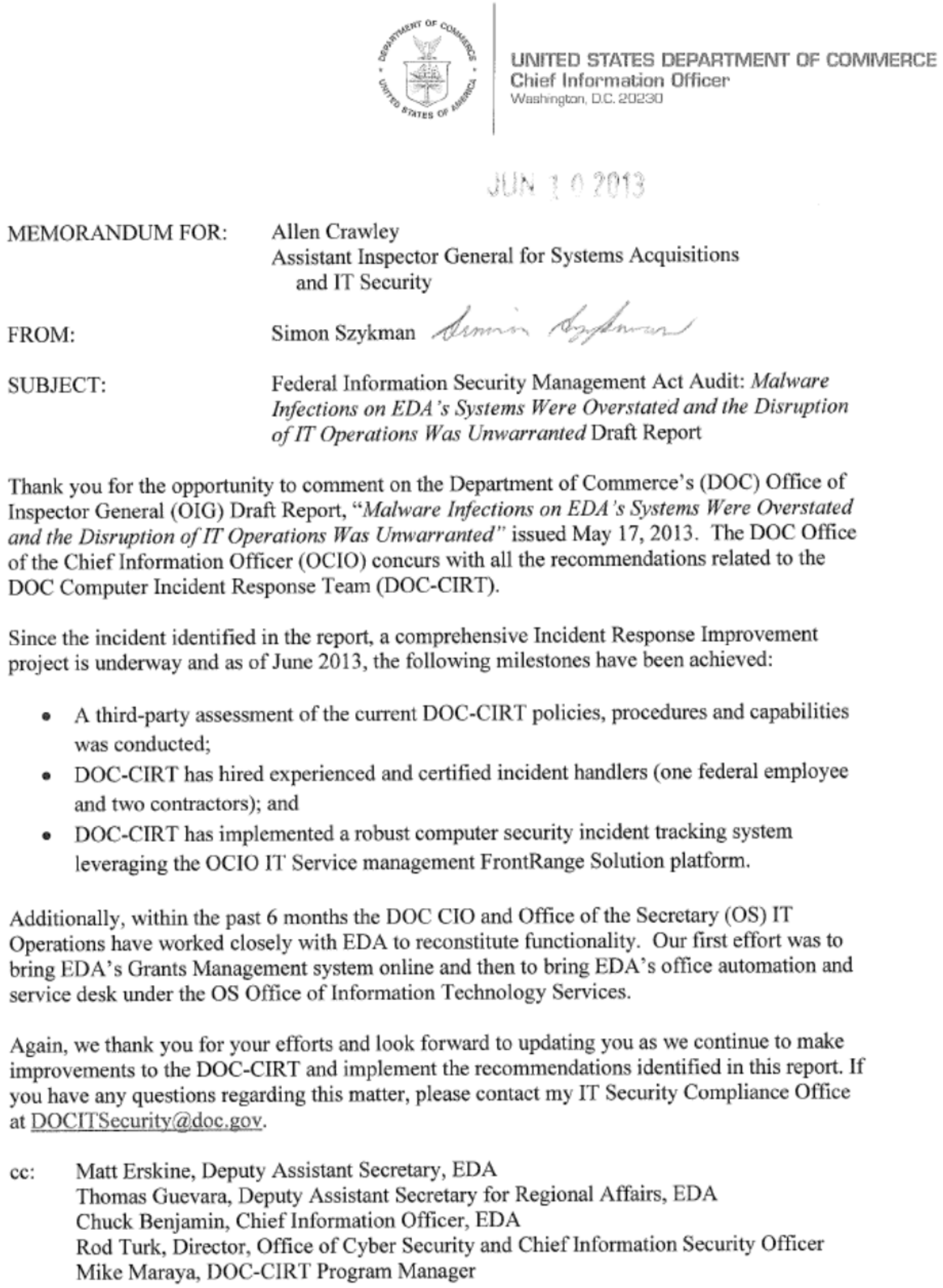
Corrective Action To Date:

In an effort to secure its IT system due to the cyber incident, EDA replaced its IT components with equipment on loan from the Bureau of the Census. Upon migration of our IT operations to the DOC HCHB network, EDA installed new equipment that had been purchased prior to the cyber incident. Prior to the cyber incident, EDA had planned to clean and surplus desktop computers and servers scheduled for replacement. As a result of this report and because very little of this equipment has been destroyed, EDA is able to continue this planned action.

Continued Action:

EDA still possesses 96 percent of its replaced inventory and intends to either put that inventory back into service or surplus the items.

Appendix D: Departmental Response



UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C. 20230

JUN 10 2013

MEMORANDUM FOR: Allen Crawley
Assistant Inspector General for Systems Acquisitions
and IT Security

FROM: Simon Szykman Simon Szykman

SUBJECT: Federal Information Security Management Act Audit: *Malware Infections on EDA's Systems Were Overstated and the Disruption of IT Operations Was Unwarranted* Draft Report

Thank you for the opportunity to comment on the Department of Commerce's (DOC) Office of Inspector General (OIG) Draft Report, "*Malware Infections on EDA's Systems Were Overstated and the Disruption of IT Operations Was Unwarranted*" issued May 17, 2013. The DOC Office of the Chief Information Officer (OCIO) concurs with all the recommendations related to the DOC Computer Incident Response Team (DOC-CIRT).

Since the incident identified in the report, a comprehensive Incident Response Improvement project is underway and as of June 2013, the following milestones have been achieved:

- A third-party assessment of the current DOC-CIRT policies, procedures and capabilities was conducted;
- DOC-CIRT has hired experienced and certified incident handlers (one federal employee and two contractors); and
- DOC-CIRT has implemented a robust computer security incident tracking system leveraging the OCIO IT Service management FrontRange Solution platform.

Additionally, within the past 6 months the DOC CIO and Office of the Secretary (OS) IT Operations have worked closely with EDA to reconstitute functionality. Our first effort was to bring EDA's Grants Management system online and then to bring EDA's office automation and service desk under the OS Office of Information Technology Services.

Again, we thank you for your efforts and look forward to updating you as we continue to make improvements to the DOC-CIRT and implement the recommendations identified in this report. If you have any questions regarding this matter, please contact my IT Security Compliance Office at DOCITSecurity@doc.gov.

cc: Matt Erskine, Deputy Assistant Secretary, EDA
Thomas Guevara, Deputy Assistant Secretary for Regional Affairs, EDA
Chuck Benjamin, Chief Information Officer, EDA
Rod Turk, Director, Office of Cyber Security and Chief Information Security Officer
Mike Maraya, DOC-CIRT Program Manager

011200000142